

REMARKS

Claims 1-14 are pending. Claims 1-14 have been rejected.

Claims 1 and 9 have been amended to further particularly point out and distinctly claim subject matter regarded as the invention.

Claims 2 and 10 have been cancelled, without prejudice.

The amendments here presented are made for the purposes of better defining the invention, rather than to overcome the rejections for patentability. Support for the amendments herein presented can be found in the specification and claims as filed. No new matter has been introduced as a result of the amendments. Reconsideration and allowance is respectfully requested in view of the amendments and the following remarks.

The 35 U.S.C. § 102 Rejection

Claims 1-14 stand rejected under 35 U.S.C. § 102(b) as being allegedly unpatentable over Nguyen (U.S. Patent No. 5,689,566). This rejection is respectfully traversed.

In the Office Action at paper number 2, paragraph 3, the Office Action asserts as to claims 1 and 9, that Nguyen shows a communication system having a checkpoint server and a router, said router having a router server a method for reconstructing separate but interrelated data comprising determining whether there has been a new connection having a corresponding base layer established through said router (request router, Nguyen, col. 2, line 64-65, col. 3, line 1-2, fig. 1 element 106). The Office Action asserts for the claim element of if there is a new connection through said router, creating a unique connection identifier (session key) for said new connection that Nguyen, discloses at col. 5, line 7-8). The Office Action asserts for the claim element of storing said corresponding base layer with said unique connection identifier therein within said

checkpoint server is disclosed at Nguyen col. 5, line 7-8, col. 11, line 41, fig. 1, element 110).

The Office Action asserts as to claims 2 and 10 that Nguyen shows claim 1 and 9 and further shows the acts of; determining whether there has been a change of state (error) for an existing connection running on said router (Nguyen fig. 2 element 106, 206, col. 7, line 43-44, col. 9, line 3); if there has been a change of state for an existing connection running on said router, then checkpointing data (packet) corresponding to said existing connection to said checkpoint server with said unique connection identifier embedded therein (Nguyen, col. 9, line 4).

The Office Action asserts as to claims 3 and 11 that Nguyen shows claim 1 and 9 and further shows the acts of determining whether there is data available within said checkpoint server for said firewall application (Nguyen, col. 2, line 57-59, col. 9, line 49); recovering said data by said firewall application from said checkpoint server if there is data available within said checkpoint server for said firewall application (Nguyen, col. 8, line 12-15, col. 9, line 49-50).

The Office Action asserts as to claims 4 and 12 that Nguyen shows a communications system having a checkpoint server a router and a firewall application, said router having a router server and at least one application module running therein, a method for reconstructing separate but interrelated data comprising; determining whether there is data (handle) available within the checkpoint server (Nguyen, col. 7, line 41-43); and recovering, by the firewall application and the at least one application module

(session write thread) (Nguyen, col. 2, line 57-59, col. 7, line 34-35, 48), said data from said checkpoint server if there is data available within said checkpoint server (Nguyen, col. 7, line 36-38, 41-42).

The Office Action asserts as to claims 5 and 13 that Nguyen shows a checkpoint server, a router, and a firewall application having at least one connection therethrough, a method for uniquely checkpointing data comprising; creating a unique connection identifier corresponding to each at least one connection through the router (session key, Nguyen, col. 5, line 7-8); checkpointing data regarding said at least one connection through said router within said checkpoint server (requester, Nguyen, col. 5, line 7-8, col. 11, line 41, fig. 1 element 110); and encoding (encrypty) said checkpointing data within said checkpoint server with said corresponding unique connection identifier (Nguyen, col. 5, line 27-28).

The Office Action asserts as to claims 6 and 14 that Nguyen shows claims 5 and 13 and further shows the acts of; recovering said checkpointing data (Nguyen, col. 8, line 12-15, col. 9, line 49-50); and reassembling said checkpointing data according to said unique connection identifier (Nguyen, col. 7, line 51-52, 55-56).

The Office Action asserts as to claim 7 that Nguyen shows communications system apparatus, having a router with connections running therethrough, the router further having a router server therein, said communications system comprising; a firewall application device running within the router, said firewall application device responsive to connections made through said router; and a checkpoint server device running within

said router, said checkpoint server device responsive to said firewall application device (Nguyen, col. 2, line 57-58, fig. 4A-C, col. 9, line 11-12), said firewall application device configured to create a unique connection identifier (session key) in response to connections made through said router (Nguyen, col. 5, line 7-8), and said firewall application device configured (Nguyen, col. 9, line 60-61) to checkpoint data associated with said connections (Nguyen, col. 5, line 28-29) with corresponding said unique connection identifier embedded therein to said checkpoint server (Nguyen, col. 5, line 7-8).

The Office Action asserts as to claim 8 that Nguyen shows claim 7 above and further shows firewall application device is further configured to recover said data from said checkpoint server (Nguyen, col. 8, line 12-15, col. 9, line 49-50) and reassembling said data using said unique connection identifier embedded within said data (Nguyen, col. 7, line 51-52, 55-56).

Applicant respectfully disagrees with the assertions in the Office Action.

To anticipate a claim under 35 U.S.C. § 102, a single source must contain all of the elements of the claim. *Lewmar Marine Inc. v. Barent, Inc.*, 827 F.2d 744, 747, 3 U.S.P.Q.2d 1766, 1768 (Fed. Cir. 1987), cert. denied, 484 U.S. 1007 (1988). Moreover, the single source must disclose all of the claimed elements “arranged as in the claim.” *Structural Rubber Prods. Co. v. Park Rubber Co.*, 749 F.2d 707, 716, 223 U.S.P.Q. 1264, 1271 (Fed. Cir. 1984).

The Nguyen reference discloses a system that uses a three way password authentication, encrypting different portions of a logon packet with different keys based on the nature of the communication link. Nodes attached to a particular LAN can have one level of security for data transfer within the LAN while data transfers between LAN's on a private network can have a second level of security and LAN's connected via public networks can have a third level of security. The level of security can optionally be selected by the user. Data transfers between nodes of a network are kept in separate queues to reduce queue search times and enhance performance. (see Nguyen at Abstract and Col. 1, lines 57-68, Col. 2, lines 1-3).

The Nguyen reference does not disclose each and every claimed element, as claimed, in claims 1, 4, 5, 7, 9, 12, or 13. The specific citations from the Nguyen reference do not anticipate each and every claimed element as claimed. The citation of (request router, Nguyen, col. 2, line 64-65, col. 3, line 1-2, fig. 1 element 106) discloses, "in a preferred embodiment, communication between a client and a server is as follows. The server waits for connection requests from clients on the network." The broad nonspecific disclosure of Nguyen does not anticipate the specific claimed elements of "a communication system having a checkpoint server and a router, said router having a router server a method for reconstructing separate but interrelated data comprising determining whether there has been a new connection having a corresponding base layer established through said router," as in claim 1 or claim 9. The citations for the remaining elements of claims 1 and 9 (i.e., Nguyen col. 5, line 7-8, col. 11, line 41, fig. 1, element 110) are also insufficient to anticipate the claimed elements. For example, the citation of

(Nguyen, col. 9, line 4) recites in full context, “If an error is detected when the packet is sent, then response signal is destroyed 342 and control is returned 344 to the application.” The citation of the Nguyen reference does not anticipate the claimed elements of “if there has been a change of state for an existing connection running on said router, then checkpointing data corresponding to said existing connection to said checkpoint server with said unique connection identifier embedded therein, wherein checkpointing is a process including critical data regarding the state of a connection through the router is stored, wherein the connection is re-established using the checkpointed data,” as claimed in part in claims 1 and 9.

The citation of (Nguyen, col. 7, line 36-38, 41-42) as applied to claims 4 and 12 does not anticipate the claimed elements of, “recovering, by the firewall application and the at least one application module, said data from said checkpoint server if there is data available within said checkpoint server,” as claimed in part in claims 4 and 12. The citation merely discloses in context, “if the resource is remote, the request router 106 first searches its local list to see if the needed communication handle is already stored in the list,” and “if the communication handle is not found in the local list, the request router 106 sends a message to the requester 110 over the request channel 12 to obtain the handle.” Thus, the citation of (Nguyen, col. 7, line 36-38, 41-42) does not anticipate the claims 4 and 12.

The citations of (session key, Nguyen, col. 5, line 7-8), (requester, Nguyen, col. 5, line 7-8, col. 11, line 41, fig. 1 element 110), and (Nguyen, col. 5, line 27-28) do not anticipate the claimed elements of “checkpointing data regarding said at least one

connection through said router within said checkpoint server and encoding said checkpointing data within said checkpoint server with said corresponding unique connection identifier,” as claimed in part in claims 5 and 13. The citations merely discloses in context, “the server saves the client initiating data, generates a session key Ks and an initializing vector IV,” “the response signals are saved in response-signal queues by the session write thread,” “after the logon procedure is successfully completed, all packet headers are encrypted using the session key K’s and the IV.” Thus, the citations of (session key, Nguyen, col. 5, line 7-8), (requester, Nguyen, col. 5, line 7-8, col. 11, line 41, fig. 1 element 110), and (Nguyen, col. 5, line 27-28), do not anticipate the claimed elements in claims 5 and 13.

The citations of (Nguyen, col. 2, line 57-58, fig. 4A-C, col. 9, line 11-12), (Nguyen, col. 5, line 7-8), (Nguyen, col. 9, line 60-61) (Nguyen, col. 5, line 28-29), and (Nguyen, col. 5, line 7-8) do not anticipate the claimed elements of, “communications system apparatus, having a router with connections running therethrough, the router further having a router server therein, said communications system comprising; a firewall application device running within the router, said firewall application device responsive to connections made through said router; and a checkpoint server device running within said router, said checkpoint server device responsive to said firewall application device, said firewall application device configured to create a unique connection identifier in response to connections made through said router, and said firewall application device configured to checkpoint data associated with said connections with corresponding said unique connection identifier embedded therein to said checkpoint server,” as claimed in

claim 7. The citations merely discloses in context, "The use of the term firewall herein refers to the requirement for increased levels of security to avoid the possibility of unauthorized data access by parties outside the organization," "Figs. 4A-C illustrate the memory layout of the packets used in the preferred embodiment. Fig. 4A illustrates a packet as encrypted by security level 1," "the server saves the client initiating data, generates a session key K_s and an initializing vector IV," "Thus thanks to the dynamic packet header technique, a user can setup different types of firewalls wherever he needs them," "after the logon procedure is successfully completed, all packet headers are encrypted using the session key K's and the IV." Thus, the citations of (Nguyen, col. 2, line 57-58, fig. 4A-C, col. 9, line 11-12), (Nguyen, col. 5, line 7-8), (Nguyen, col. 9, line 60-61) (Nguyen, col. 5, line 28-29), and (Nguyen, col. 5, line 7-8) do not anticipate the claimed elements in claim 7.

Since the prior art reference fails to disclose each and every claimed element, then the prior art reference fails to anticipate the claimed invention. In view of the foregoing, it is respectfully requested that the rejection be withdrawn and it is respectfully asserted that the claims are now in condition for allowance.

Dependent Claims

The argument and evidence set forth above is equally applicable here. Since the independent Claims 1, 5, 7, 9, and 13, are allowable, then the dependent Claims 3, 6, 8, 11, and 14 must also be allowable. If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596 (Fed. Cir. 1988).

In view of the foregoing, it is respectfully requested that the rejection be withdrawn and it is respectfully asserted that the claims are now in condition for allowance.

Prior art made of record

The Office Action cited prior art of record but did not rely upon the prior art. Applicants have considered the prior art made of record and assert that the claimed invention is patentably distinct over prior art made of record.

Request for Allowance

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

Respectfully submitted,
SIERRA PATENT GROUP, LTD.

Dated: *March 17 2004*


Andrew D. Gathy
Reg. No.: 46,441

Sierra Patent Group
P.O. Box 6149
Stateline, NV 89449
(775) 586-9500